FARMINGTON POLICE DEPARTMENT

POLICY AND PROCEDURE

	Policy Number: 251-01	**Effective Date:** 11/11/2016
	Subject: Criminal Intelligence	
	Approved by: **Steven D. Hebbe, Chief of Police**	

PURPOSE:

To establish guidelines for the collection and dissemination of criminal intelligence information and maintenance of a Criminal Intelligence System.

POLICY:

It is the policy of the Farmington Police Department to collect criminal intelligence information and to disseminate it to divisions within the department in order to prevent, solve, and reduce criminal activity. It is the policy of the Farmington Police department to maintain a Criminal Intelligence System in compliance with Federal Regulations.

PROCEDURE:

It is the responsibility of every officer to obtain and distribute criminal intelligence through formal and informal avenues. Through the use of the Farmington Police Department intranet, employees post criminal intelligence, such as stolen vehicles, wanted persons, and attempt to locates, and close patrols. At the beginning of their shift, each officer is expected to review new information posted on the intranet.

The shift supervisor, or his designee, briefs the next shift on significant events and persons of interest that occurred during the shift.

The Farmington Police Department uses a briefing board in the distribution of information on wanted persons and other criminal activity. By posting items on the briefing board, officers may request assistance, such as the identification of suspects, on current criminal investigations.

Through the use of briefing training and other training avenues, officers receive training on the proper handling and dissemination of criminal intelligence. Criminal intelligence should be treated as confidential information and should only be accessible to qualified individuals.

For formal and long term criminal intelligence, the Farmington Police Department Criminal Intelligence System is maintained at the direction of the Detective Lieutenant. Our system is maintained to assist officers in criminal investigations and ensure that the collection, dissemination, and management of Criminal Intelligence conforms to privacy laws and the constitutional rights of individuals. Procedures for the utilization of Criminal Intelligence must meet all requirements of 28 Code of Federal Regulations (CFR) Part 23.

Definition of Criminal Intelligence File:

A Criminal Intelligence File consists of stored information on the activities and associations of:

1. Individuals who:

   a. Are suspected of being involved in the actual or attempted planning, organizing, financing or commission of criminal acts; or

   b. Are suspected of being involved in criminal activities with known or suspected crime figures.

2. Organizations, businesses, and groups that:

   a. Are suspected of being involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or

   b. Are suspected of being operated, controlled, financed, or infiltrated by known or suspected crime figures for use in illegal activities.

File Content:

Only information with a criminal predicate which meet the defined criteria for file input should be stored in the criminal intelligence file. Specifically excluded material includes:

1. Information on an individual or group merely on the basis that such individual or group support unpopular causes;

2. Information on an individual or group merely on the basis of ethnic background;

3. Information on any individual or group merely on the basis of religious or political affiliations;

4. Information on an individual or group merely on the basis of non-criminal personal habits;

5. Criminal Records should be excluded from an intelligence file;

6. Also excluded are associations with individuals that are not of a criminal nature.

File Criteria:

Criteria for Permanent status in the Criminal Intelligence File (Five Year):

1. Information that relates to an individual, organization, business, or group that is suspected of being involved in the actual or attempted planning, organizing, financing, or committing of one or more of the following criminal acts:

   a. Narcotic trafficking or manufacturing;

b. Extortion;

c. Vice and Pornography;

d. Infiltration of legitimate business for illegitimate purposes;

e. Stolen Securities;

f. Bribery;

g. Major crimes including homicide, sexual assault, burglary, auto theft, kidnapping, destruction of property, robbery, fraud, fencing stolen property and arson;

h. Manufacture, use, or possession of explosive devices for purposes of fraud, intimidation, political motivation, homicide, or related crimes and destruction of public or private property;

i. Threats to public officials and private citizens;

j. Corruption of public officials.

2. In addition to falling within the confines of one or more of the above criminal activities, the subject/entity to be given permanent status must be identifiable-distinguished by a name and unique identifying characteristics (including date of birth, criminal identification number, driver's license number, or address). Identification at the time of the file input is necessary to distinguish the subject/entity from existing file entries and those that may be entered at a later time. The exception to this would be modus operandi files. Modus operandi files may be retained indefinitely while additional identifiers are sought.

Criteria for Temporary Status in the Criminal Intelligence File (One Year):

Information that does not meet the criteria for permanent storage but may be pertinent to an investigation involving one of the categories previously listed should be given "temporary" status. Retention of temporary information should not exceed one year unless a compelling reason exists to extend this time period. (For example: if several pieces of information indicate that a crime has been committed, but more than one year is needed to identify a suspect). If the information is still classified as temporary at the end of a one year period, and a compelling reason for its retention is not evidence, the information should be purged. An individual, organization, business, or group may be given temporary status in the following cases:

1. Subject/entity is unidentifiable- the subject/entity, although suspected of being engaged in criminal activities, has no corroborating identification numbers;

2. Involvement is questionable- involvement in criminal activities is suspected by a subject/entity which has either:

a. Possible criminal associations- individual, organization, business or group (not currently reported to be criminally active) associates with a known criminal and appears to be jointly involved in illegal activities;

b. Criminal history- individual, organization, business, or group) not currently reported to be criminally

active) that has a history of criminal conduct, and the circumstances currently being reported indicates they may become criminally active.

3. Reliability/validity unknown- the reliability of the information sources and/or the validity of information cannot be determined at the time of receipt; however the information appears to be significant and merits temporary storage while verification attempts are made.

When an officer obtains intelligence that qualifies as information to be entered in to the Criminal Intelligence File, the officer shall submit a memorandum to the Detective Lieutenant or his designee with as detailed and specific information as possible. That information is then evaluated.

Evaluation of information:

Information to be retained in the criminal intelligence file should be evaluated and designated for reliability and content validity prior to filing.

The bulk of the data an intelligence unit receives consists of unverified allegations or information. Evaluating the information's source and content indicates to future users the information's worth and usefulness. Circulating information which may not have been evaluated, where the source reliability is poor and content validity is doubtful, is detrimental to our agency's operations and contrary to the individual's right to privacy. To ensure uniformity with the intelligence community, stored information should be evaluated according to the criteria set forth below:

1. Source reliability:

   a. Reliable- The reliability of the source is unquestioned or has been well tested in the past.

   b. Usually Reliable- The reliability of the source can usually be relied upon as factual. The majority of information provided in the past has been proved to be reliable.

   c. Unreliable- The reliability of the source has been sporadic in the past.

   d. Unknown- The reliability of the source cannot be judged. Its authenticity or trustworthiness has not yet been determined by either experience or investigation.

2. Content Reliability:

   a. Confirmed- The information has been corroborated by an investigator or another independent, reliable source.

   b. Probable- The information is consistent with past accounts.

   c. Doubtful- The information is inconsistent with past accounts.

   d. Cannot be judged- The information cannot be judged. Its authenticity has not yet been determined by either experience or investigation.

Information Classification:

Information retained in the criminal intelligence files should be classified in order to protect sources, investigations, and the individual's right to privacy. Classification also indicates the internal approval which must be completed prior to the release of information to persons both within and outside the department. However, the classification of information itself is not a defense against a subpoena duces tecum.

The classification of criminal intelligence information is subject to continual change. The passage of time, the conclusion of investigations, and other factors may affect the security of classification assigned to particular documents. Documents within the intelligence files should be reviewed on an ongoing basis to ascertain whether a higher or lesser degree of document security is required to ensure that information released when and if appropriate.

Classifications include:

1. Sensitive:

   a. Information pertaining to significant law enforcement investigations;

   b. Corruption (police or other government officials) or other sensitive information;

   c. Informant identification information;

   d. Criminal intelligence reports which require strict dissemination and release criteria.

2. Confidential:

   a. Criminal intelligence reports not designated as sensitive;

   b. Information obtained through intelligence channels that are not classified as sensitive and is for law enforcement use only.

3. Restricted:

   a. Reports that at an earlier date were classified sensitive or confidential and the need for high-level security no longer exist.

   b. Non-confidential information prepared by/for law enforcement agencies.

4. Unclassified:

   a. Civic-related information to which, in its original form, the general public had direct access (i.e., public record data).

   b. News media information- newspaper, magazine, and periodical clippings dealing with specified criminal categories.

Information Source:

In all cases, source identification should be available in some form. The true identity of the source should be

used unless there is a need to protect the source.

The value of information stored in criminal intelligence files is often directly related to the source of such information. Some factors to consider in determining whether source identification is warranted include:

1. The nature of the information reported;

2. The potential need to refer to the source's identity for further prosecutorial activity;

3. The reliability of the source.

Whether or not confidential source identification is warranted, reports should reflect the name of the agency and the reporting individual. In those cases where identifying the source by name is not practical for internal security reasons, a confidential informant number may be used. A confidential listing of coded sources of information can then be retained by the Detective Lieutenant or designated Sergeant. In addition to identifying the source, it may be appropriate in a particular case to describe how the source obtained the information.

Information Quality Control:

The Detective Lieutenant, or designated Sergeant should conduct a thorough review for compliance with established file input guidelines and policy prior to Criminal Intelligence information being filed. The review should include ensuring that all information entered into the criminal intelligence files conforms to the file criteria and has been property evaluated and classified.

File Dissemination:

Information from a criminal intelligence report can only be released to an individual who has demonstrated both a "need-to-know" and a "right to know."

"Right to know"- Requestor has official capacity and statutory authority to the information being sought.

"Need to know"- Requested information is pertinent and necessary to the requestor agency in initiating, furthering, or completing an investigation.

No "original document" which has been obtained from an outside agency is to be released to a third agency. Should such a request be received, the requesting agency will be referred to the submitting agency for further assistance. Stored information shall be classified according to the following:

SECURITY LEVEL	DISSEMINATION	CRITERIA RELEASE AUTHORITY
Sensitive	Restricted to Law Enforcement personnel having a specific need to know and right to know.	Detective Lieutenant
Confidential	Same as Sensitive	Detective Lieutenant or Designated Sergeant
Restricted	Same as Sensitive	Law Enforcement Officer
Unclassified	Non-restricted personnel	Law Enforcement Personnel

The integrity of the criminal intelligence file can be maintained only by strict adherence to proper dissemination

guidelines. To eliminate unauthorized use and abuse of the system, a record of dissemination and requests for dissemination of information should be maintained with each stored document. Release of the document should note the date of the request, the name of the agency and individual requesting the information, the need to know, the information provided, and the name of the employee handling the request.

File Review and Purge:

File Review:

Information stored in the criminal intelligence file should be reviewed periodically for reclassification or purge in order to:

1. Ensure that the file is current, accurate, and relevant;
2. Safeguard the individual's right to privacy as guaranteed under federal and state laws;
3. Ensure that the security classification level remains appropriate.

Purge Criteria:

General considerations for reviewing and purging information stored in the criminal intelligence file are as follows:

1. Utility:
    a. How often is the information used?
    b. For what purpose is the information used?
    c. Who uses the information?
2. Timeliness and Appropriateness:
    a. Is this investigation still ongoing?
    b. Is the information outdated?
    c. Is the information relative to the needs and objectives of the agency?
    d. Is the information relevant to the purpose for which it was collected and stored?
3. Accuracy and Completeness:
    a. Is the information still valid?
    b. Is the information adequate for identification purposes?

c. Can the validity of the data be determined through investigative techniques?

Review and Purge Time Schedule:

Reclassifying and purging information in the intelligence file should be done on an ongoing basis as documents are reviewed. In addition, a complete review of the criminal intelligence file for purging purposes should be undertaken periodically. This review and purge schedule can vary from once each year for documents with temporary status to once every five years for permanent documents.

Manner of Destruction:

Material purged from the criminal intelligence file should be destroyed. A secure method of disposal is used for all records or papers that identify a person by name.

File Security:

Criminal intelligence files are maintained on an electronic storage media in a secure location designated by the Detective Lieutenant. Access to this storage media is limited to the Detective Lieutenant or designated Sergeant. Files rated as unclassified may be stored on our AS400 computer system. Access to this portion of the AS400 is limited to law enforcement personnel.

Responsibilities of Agency Personnel:

It is the responsibility of all agency personnel to identify criminal intelligence and to collect the appropriate information to be submitted into the Criminal Intelligence Data Base.

Submission of criminal intelligence information should be completed by documenting the information obtained and forwarding it to the Detective Lieutenant via secure email or by submission of a Criminal Intelligence Card.

Criminal Intelligence Cards should be submitted to a secured box located in the area of Patrol Briefing. The Detective Lieutenant or designated Sergeant has access to this secured box. After information from the Criminal Intelligence Card is entered into the data base by the Detective Lieutenant or designated Sergeant, the Criminal Intelligence Card is destroyed.

Training of Agency Personnel:

Agency personnel are trained in the Criminal Intelligence function and are encouraged to document information gleaned from a variety of sources. Training is conducted annually and includes a review of this policy by all personnel.

Annual Review of Procedures and Processes:

An Annual Review of Procedures and Processes is conducted by the Detective Lieutenant or designated Sergeant.